applied sciences

MDPI

Article

A Localized Bloom Filter-Based CP-ABE in Smart Healthcare

Krishna Priya Remamany [1], K. Maheswari [2], C Ramesh Babu Durai [3], N. K. Anushkannan [4], D. Rosy Salomi Victoria [5], Mohamed Tahar Ben Othman [6,7,*], Monia Hamdi [8] and Habib Hamam [9,10,11,12]

1 Department of Engineering-Electrical Section, University of Technology and Applied Sciences, Shinas Campus, Shinas 324, Oman
2 Department of Computer Science and Engineering, CMR Technical Campus, Kandlakoya, Hyderabad 501401, India
3 Department of Electronics and Communications Engineering, Dhanalakshmi College of Engineering, Manimangalam, Tambaram, Chennai 601301, India
4 Department of Electronics and Communication Engineering, Kathir College of Engineering, Neelambur, Coimbatore 641062, India
5 Department of Computer Science and Engineering, St. Joseph's College of Engineering, Chennai 600119, India
6 Department of Computer Science, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia
7 Spectrum of Knowledge Production & Skills Development, Sfax 3027, Tunisia
8 Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
9 Faculty of Engineering, Uni de Moncton, Moncton, NB E1A 3E9, Canada
10 International Institute of Technology and Management, Commune d'Akanda, Libreville P.O. Box 1989, Gabon
11 School of Engineering, Canadian Institute of Technology, Kompleksi Xhura, Rruga Xhanfize Keko 12, 1000 Tirana, Albania
12 School of Electrical Engineering, Department of Electrical and Electronic Engineering Science, University of Johannesburg, Johannesburg 2006, South Africa
* Correspondence: mtothman@gmail.com

Citation: Priya Remamany, K.; Maheswari, K.; Ramesh Babu Durai, C.; Anushkannan, N.K.; Victoria, D.R.S.; Ben Othman, M.T.; Hamdi, M.; Hamam, H. A Localized Bloom Filter-Based CP-ABE in Smart Healthcare. *Appl. Sci.* **2022**, *12*, 12720. https://doi.org/10.3390/app122412720

Academic Editor: Nuno Silva

Received: 7 November 2022
Accepted: 30 November 2022
Published: 12 December 2022

Abstract: Wearable technology-supported cloud-based smart health (s-health) has emerged as a promising answer to increase the efficiency and quality of healthcare as a result of rapid improvements in Internet of Things (IoT) technologies. However, the issues of data security and privacy preservation have not been fully resolved. In recent years, ciphertext policy attribute-based encryption (CP-ABE), which was developed as a versatile and potent cryptographic fundamental to accomplish one-to-many encryption with fine-grained access control, has been seen as a viable answer to the security issue in the cloud. The attribute values in the access policy, however, are supplied in cleartext in standard CP-ABE. This will conveniently reveal the data owners' privacy (patients). Because the Internet of Things (IoT) in healthcare stores sensitive data in the cloud, security is crucial. The data must always be accessed via an access key when using traditional encryption techniques. Though the data cannot be accessed right away in an emergency, this offers greater security. The healthcare IoT created the break-glass concept to address this. The encryption technique is integrated with the broken glass idea to offer data protection and simple access in emergency scenarios. The majority of research papers employ cypher text policy attribute-based encryption (CP-ABE) with the broken glass idea to secure electronic health records. For improving data accessibility in the smart healthcare environment, modified cypher text policy attribute-based encryption (MCP-ABE) with the broken glass (BG) technique is suggested. Greater information security is achieved with this method, but the access policy is also dependent on keys that are vulnerable to hacking. To analyze the access policy individually throughout the key generation process, the attribute-based encryption procedure in this case uses the bloom filter. Information about the access policy is kept intact, which enhances the security of the keys. To continue serving patients and saving their lives, this modified CP-ABE is integrated with break glass in the smart healthcare facility. The experimental results demonstrated that, when compared to the lightweight break-glass procedure, the proposed solution is likewise the best in terms of decreased overhead. The main benefit of this strategy is that it uses the bloom filter concept in the MCP-ABE process, which protects the access policy attributes, to ensure that the key is never compromised. For data access in smart healthcare to preserve patients' lives, the proposed MCP-ABE with broken glass is best.

Keywords: smart healthcare; encryption; bloom filter; break glass; security; data preserving

1. Introduction

The internet and the Internet of Things are the biggest boons to civilization in today's world. Both of these methods allow authenticated users and their owners to access their data remotely. Based on this, the IoT is used in the healthcare sector for the close monitoring of patients by doctors.

In healthcare IoT, security is a must because it saves confidential data in the cloud. Traditional encryption algorithms necessitate the use of an access key at all times to access the data. This provides greater security, but in an emergency, the data cannot be accessed immediately. To overcome this, the break-glass concept was introduced in healthcare IoT. In the break-glass (BG) method, the secured data can be accessed only once without any login credentials. [1] This helps in an emergency, but provoking BG is an important task. In this section, the techniques used in healthcare IoT for security are discussed. A survey on techniques used for securing the data in the Internet of Things is discussed in [2]. The four-phase authentication process is proposed between the server and local processing unit for securing the data transmission in the body sensor network [3]. A Datagram transport layer security handshake (DTLS-H) mechanism and session-oriented data access scheme are proposed in [4]. Here, the DTLS-H is used to create the authentication and data transmission process between the users in fog computing-based healthcare IoT. This approach is better in all terms such as security, computation, and storage overhead in data transferring between users. A survey of security mechanisms used for various applications in the IoT domain is discussed in [5]. Most of the existing methods in IoT utilized the two-stage authentication scheme. This approach is not sufficient for third-party storage data. To overcome this, [6] proposed a biometric-based authentication scheme for each layer of the IoT process. Here, they utilized a face recognition scheme for data access in four layers of the IoT process. They combined face recognition with bilinear cryptography to prevent data leakage in each layer. This approach provides high security compared to traditional approaches. However, the authenticated user also cannot access data when they face any accidents or injuries. A session-oriented hash lock and key-based communication access protocol are proposed in [7]. Here, two types of keys are generated during the communication between devices: the random key and the session key. The random key is used for authentication and the session key is used for authenticating the data transmission and analyzing the presence of intruders in the communication. The hash lock scheme is used to secure the data during the transmission process. A survey of smart healthcare management using wearable sensors and IoT is presented in [8]. Here, smart healthcare architecture, communication protocols, and security issues are discussed. Based on their survey, the modifications in attribute-based encryption and fully homomorphic encryption are suitable for improving security in IoT. An end-to-end security mechanism is proposed for Internet of Things applications [9]. Here, the authentication is performed using the Advanced Encryption Standard Galois Counter Mode (AES-GCM) 256-bit and one-pass scheme. The authentication between the base station and users is performed using hash key generation. A Secure Authentication and Prescription Safety protocol is proposed for healthcare IoT [10]. Here, efficient elliptical cryptography is proposed for securing data transmission between all parties, such as nurses, doctors, and patients. This approach performed well against the attacks, but the symmetric key system with single cryptography results in data leakage during third-party storage. A survey on data access mechanisms and attacks in the healthcare environment is discussed in [11]. Based on that, a secured scheme is proposed for both the cloud and healthcare local data. The Shamir secret sharing scheme is used in [12] to protect electronic health records. Here, the reconstruction of the record from shared messages is performed using cloud operators to save computational time and complexity for both healthcare centers and patients. This approach preserves both time

and data in smart healthcare IoT. A real or random model is proposed in [13] for generating the session key for data storage in the cloud. This key is generated after the successful access of the user's wearable device to the cloud. This approach performs well on both the computational and security side for session key protection. In healthcare IoTs, many techniques are used to encrypt and access data [14]. For accessing the data, depending on their responsibilities, attribute-based encryption is used. The information is protected through the group key and it is also transferred and verified through a key matching policy based on their roles. Surveys of security mechanisms used by wearable devices for storing information in the cloud are discussed in [15]. It states that most devices utilize a short-term privacy policy for protecting the data, and this needs to be updated during healthcare monitoring. The recent techniques used in healthcare IoT and their shortcomings are discussed in the following section. The paper is organized as follows. Section 2 highlights the techniques combined with the break-glass procedure in smart healthcare units. Section 3 briefly explains the proposed methodology and its security analysis. Section 4 compares the proposed method performance with the existing lightweight break access. Finally, the paper is concluded with a summary in Section 4.

2. Proposed Method

In this paper, modified cipher text policy attribute-based encryption (MCP-ABE) with a break-glass (BG) mechanism is proposed for data access in the smart healthcare environment. The architecture diagram of the smart healthcare environment is shown in Figure 1.

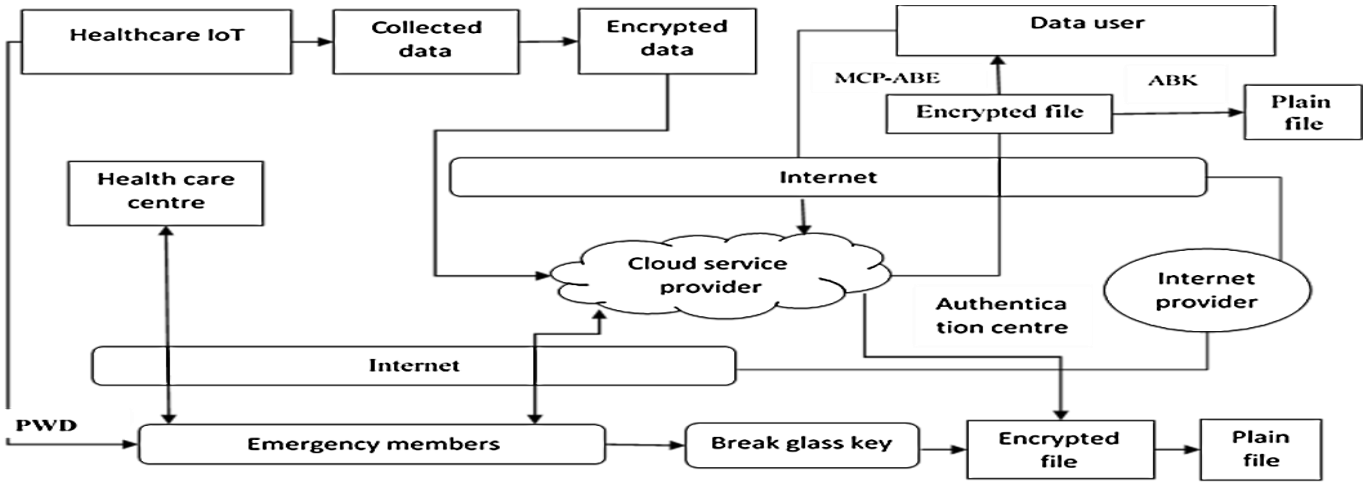

Figure 1. Proposed model architecture.

2.1. Architecture Components

Figure 1 shows the architecture of the proposed MCP-ABE-BG in a smart healthcare system. Here, the following units are essential blocks in the proposed system:

- Authorization center;
- Cloud service provider;
- Healthcare center;
- Patients;
- Emergency contact member;
- Users.

In the authorization center (AC), the user registration and key generation for both modified CP-ABE and break glass operation is performed. Here, the public key is shared with all users and the private key is preserved with individual users to access the data based on their needs. A cloud service provider (CSP) is a storage system used to store patient information from healthcare centers. The healthcare center (HC) is a smart environment in

which the devices are interconnected through the internet to read and write the information to the CSP based on their access level. The patients (P) are the persons who utilize the resources provided by HC to cure their disease. The emergency contact member is the first-line helper assigned by the patient to access the encrypted information during an emergency scenario. Users are doctors, nurses, friends, or relatives of the patients who can access the data through their access policy for patient welfare.

2.2. Security Model

In this paper, the full security mode of indistinguishable against chosen plaintext attack is proposed for providing security to the modified CP-ABE. The access policy is also fully protected in the transmission mode, while in the selective approach, the policies are protected at the beginning stage only. Hence, the fully secured model is used to preserve the access policies at all times. The proposed algorithm should satisfy the following conditions to provide better security for electronic health records. The passwords from AC should not be accessed or detected by the CSP and HC from the stored information. Even in the BG process, the enterprise content management system (ECM) stores its password in an encrypted format to prevent access from CSP and HC.

2.3. MCP-ABE Workflow

Two types of access schemes are used for data retrieval from the cloud. One is normal access through modified CP-ABE access based on its attributes. The other is the break-glass access that is provoked during an emergency situation by ECM to save the patient. These two types of access schemes are explained below.

Dual-Access Scheme

The dual-access scheme is performed through the different processes as follows: setup, key generation, bloom filter setup, encryption, bloom filter reconstruction, decryption, break-glass key generation, and extraction, as shown in Figure 2.

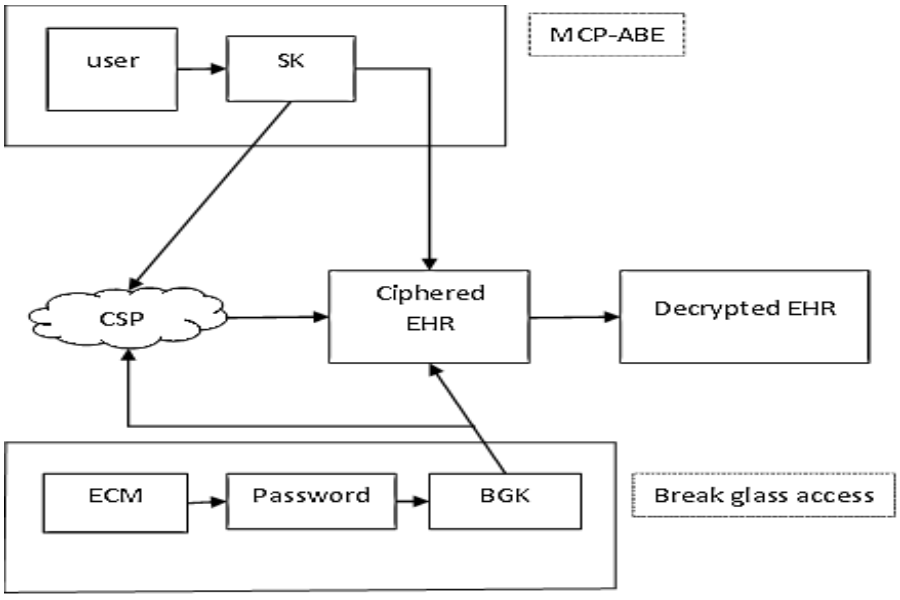

Figure 2. Dual access.

In MCP-ABE, the users are registered through the authorization center and receive the secret key (SK). Using the SK, the ciphered electronic health record is obtained from the cloud service provider (CSP). Here, the secret key cannot be hacked because it is not combined with the access policy. This will be checked during the bloom filter reconstruction process. The final decryption of the document is performed using the secret key in the healthcare unit, as shown in Figure 2.

During emergencies, the break-glass access is revoked, as shown in Figure 2. Here, the ECM utilizes the password obtained from the patient to generate the break-glass key. After generating the break-glass key (BGK), BGK1 and BG2 are used to obtain the cipher document from CSP or HC, respectively, as shown in Figure 3.

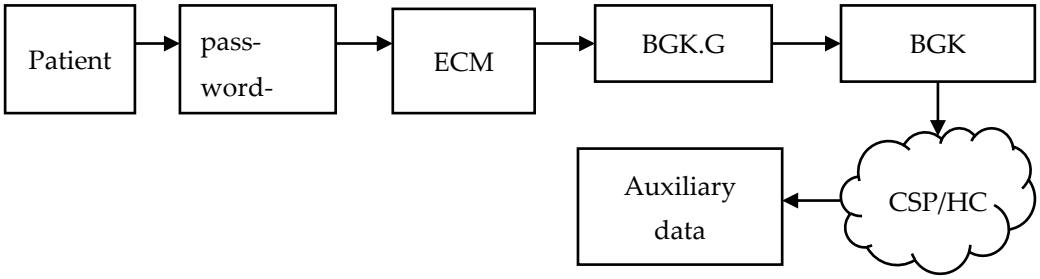

Figure 3. Break-glass key (BGK) generation.

The BGK and password are used to perform the decryption process, as shown in Figure 4. By performing this process, the ciphered document is accessed without a primary user and updates the information during its session period. This helps to save the patient's life and keep track of their health conditions continuously.

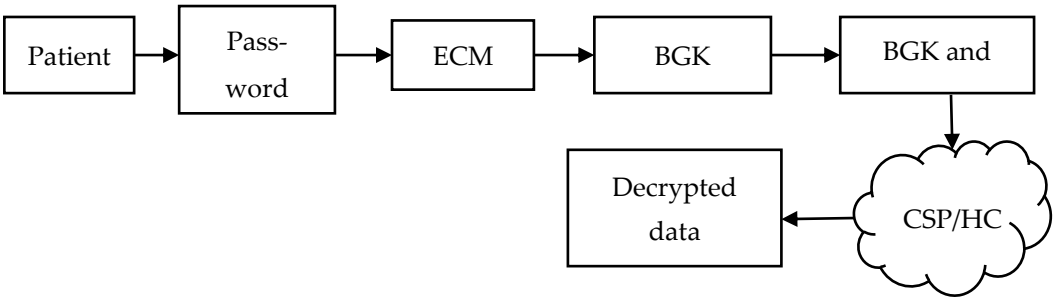

Figure 4. Break glass key extraction.

2.4. Proposed Method Process

The detailed steps in the proposed MCP-ABE-BG for a smart healthcare environment are as follows.

2.4.1. Setup

The public key (PK) and master key for the whole operations are generated using the random parameter q or the attributes. The authorization center performs these operations using the following parameters. Let A be the total attributes, and maximum length is denoted by AL. The bloom filter length is BFL and the maximum row size length is RL. The number of the hash function is denoted by NH. The two cyclic multiplicative groups are indicated using MG and MG'. The bilinear map for this multiplicative group is as follows:

$$BM = MG * MG' \tag{1}$$

For a randomly selected generator 'G', the PK and master key (MK) from the setup is as follows:

$$MK = G^{alpha} \tag{2}$$

The public key is given as follows:

$$PK = \left\{ G,\ BM(G,G)^{alpha}, G^{a},\ A_L,\ BF_L,\ R_L,\ r_1, r_2, \ldots\ r_l,\ H_{1(\ )},\ H_{NH} \right\} \tag{3}$$

Here, the H indicates the hash functions, r indicates the random group elements from the attributes, and BM indicates the bilinear matrix.

2.4.2. Secret Key Generation

The secret keys for the electronic health records are generated based on the attributes mentioned by the users. Here, the secret key SK is generated using public key (PK), master key (MK), and the attribute set (A). The key (K) generator matrix using generator (G) is as follows in Equation 4.

$$K = G^{a} * G^{at} \tag{4}$$

The other attributes such as length and hash functions for generating the secret key are given in Equations (5)–(7).

$$L = G^{t} \tag{5}$$

$$K_x = G_x^t, \ \ x \ \in \ A \tag{6}$$

$$SK = \{K, L, K_x, \ A\}, \ \ t \in \ ZP \tag{7}$$

Here, the term ZP indicates the linear variable to indicate the fine grain access for all users using linear secret sharing of the master key in MCP-ABE.

2.4.3. Encryption

Encryption is performed after verifying the attributes in the bloom filter process. First the encryption, and then the bloom filter setup, are run to indicate the selected attributes from the access policy for the encryption process. The working of this process is given in the following Algorithms 1 and 2.

The algorithm for encryption is given below.

Algorithm 1: Encryption

Input: Master key MK, Electronic health record (EHR), (MG, ρ), Access matrix MG = l * n
Output: Ciphered EHR (C-EHR)
Begin
Initialize encryption secret $S, \ S \in \ ZP$
For i = 1: l
$\lambda_i =$ MiV
$\mathrm{C-EHR} = \{\mathrm{C} \ = \ \mathrm{EHR}. \ BM^{'(G,G)^{alpha*s}}, C' = G^{s}[\ C_i = g^{a\lambda i} * h^{-s}{}_{\rho(\mathrm{i})}\ ]\mathrm{i} = 1 \ldots \mathrm{l}$
End
End

λ_i is used to localize the selected attributes in the access policy MG. Here, the EHR is only encrypted and the access policy is not combined with it. It is sent to the CSP through bloom filter output, as shown in Algorithm 2.

Using the above algorithm, the attribute selection process is performed in the modified ABE. Using this BF output and the secret key, the data are encrypted in the CSP or HC and shared among them. The selected attribute is mentioned by indexing through a localization pointer in an array format.

The whole attribute set is indicated as a vertical row. The attributes selected for encryption are highlighted through a localization pointer, as shown in Figure 5.

Algorithm 2: Selected Attributes Using BF

Input: MG, ρ—selected attributes.
Output: BFO
Begin
Selected attributes Ae from (MG, ρ)
BFO create for 'n' attributes
For I = 1: n
BFO[i] = 0;
For each e in Ae
R = 1;
S = x;
For i = 1: K (hash function)
K1 = Hi + 1 (Ae)
If BFO[K1] == 0
If R == −1
J = P
Else
Random strings $r_{J,e}$ produced
ABF [J] == $r_{J,e}$
S = S ⊕ ABF [J]
End
Else
S = S ⊕ ABF [J]
End
ABF [S] = S
End
End
For I = 1: n
If BFO [i] == 0
BFO [i] = random number
End
End
End

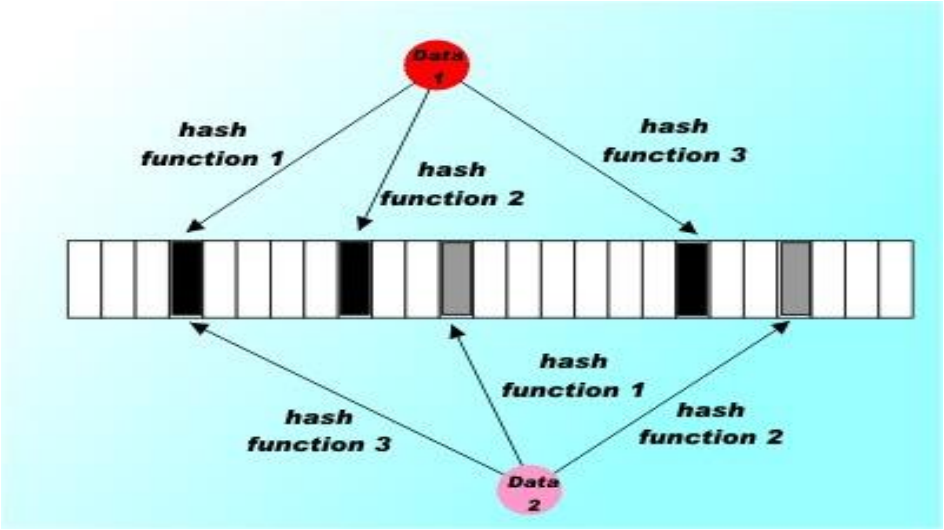

Figure 5. Bloom filter access.

2.4.4. Decryption

In the traditional process, the decryption is simple as the ciphered records contain the access policy. However, the access policy is separated from the ciphered record. Hence, the

attribute extraction is performed first, and then the decryption process is performed. The Algorithm 3 for this process are given below.

Algorithm 3: Attribute Extraction Using BF Reconstruction

Input: S—user-selected attributes. BFO—bloom filter output. PK—public key
Output: Mapped attributes ρ′
Begin
For each selected attribute at in S
$RS = \{0\}^{\lambda}$
For i = 1: k
J = Hi + 1 (at)
RS = RS $\oplus$ ABF [J]
Ae = RS[LSB]
remove lead zeros in Ae
if Ae = at
rn =RS[MSB]
remove lead zeros in rn
End
ρ′= [urn, Ae]
end
end

Here, the attribute mapping is performed using the doctor-selected attributes and the bloom filter output to identify the row number (rn) in the total attribute set (ae). With these mapped attributes, the ciphered text is decrypted using the following Algorithm 4.

Algorithm 4: Decryption

Input: Secret key SK, C-EHR, MG, ρ′, K- hash functions
Output: EHR
Begin
If ρ′ is satisfied

$$s = \sum_{i \,\epsilon I} C_i * \lambda_i$$

$$e'(g,g)^{as} = e'(C',K) / \prod_{i \,\epsilon I} e'(C_i, L)\, e'\left(C', K_{\rho'(i)}\right)$$

$$EHR = C - EHR / e'(g,g)^{as}$$

Else
EHR = null value
End
End

Using these two algorithms, the ciphered electronic health records are decrypted. The decryption cannot be easily performed; this helps to improve the data confidentiality, compared to the traditional ABE.

2.4.5. Break-Glass Key Generation

Break-glass key generation occurs during the emergency scenario by using the shared password from patients to ECM. Here, the shared password (PW) helps to generate the break-glass key using the following Algorithm 5.

Using Algorithm 5, the break-glass keys are generated by the ECM using a shared password. With these keys, the data can be extracted during emergency times.

Algorithm 5: Break-Glass Key Generation

Input: shared password PW, linear gain matrix ZP, and generator matrix G.
Output: BGK, BGK1 and BGK2
Begin
Initialize Random value R1, R2 R1, $R2 \in ZP$
Select Break glass Key K and CSP key K1 K, $K1 \in G$
Select theta 1 from ZP

$$P_{CSP} = G_1{}^{theta1}$$

Select theta 2 from ZP

$$P_{HC} = G_2{}^{theta2}$$

Calculate K2 for HC using following equation

$$K2 = K \cdot \frac{1}{K1} \cdot (P_{CSP} \cdot P_{HC})^r$$

Calculate key factors for CSP and HC using following equation

$$CSP = (P_{CSP})^{-2r2} \cdot G_1^{-r}$$
$$HC = (P_{HC})^{-2r1} \cdot G_2^{-r}$$

Calculate BGK for CSP and HC using following equations

$$BGK1 = (K1,\ CSP)$$
$$BGK2 = (K2,\ HC)$$

End

2.4.6. Break-Glass Key Extraction

In this, the ECM sends a break-glass request to CSP or HC. Once this request is sent, the password for CSP and HC from Algorithm 5 is sent to the ECM. The ECM performs the operations in Algorithm 6 to extract the final key.

Algorithm 6: Break-Glass Key Extraction

Input: P_{CSP}, P_{HC}, *patient identiy*, PW and other parameters used from CSP and HC
Output: BGK
Begin
Select s from ZP
Calculate R using

$$R = H1(patient\ identiy,\ PW)$$

Calculate r1 and r2

$$r1 = (P_{CSP})^R \cdot G_1^{-s}$$
$$r2 = (P_{HC})^R \cdot G_2^{-s}$$

From r1 and r2 calculate bgk1 and bgk2
$bgk1 = K1 \cdot (R1 \cdot r1)^{theta\ 1}$ in CSP
$bgk2 = K2 \cdot (R2 \cdot r2)^{theta\ 2}$ in HC
Final BGK is as follows

$$BGK = (\ bgk1 \cdot bgk2) \cdot (P_{CSP} \cdot P_{HC})^{-s}$$

End

From this algorithm, the break-glass key for extracting the ciphered EHR is obtained, and it is decrypted on the destination side. Using this process, the MCP-ABE-BG is implemented in a smart healthcare IoT system.

2.5. Security Analysis

For security analysis, ABE is used, which is the best encryption algorithm, as plain text cannot be accessed. At the most, the access policy is verified using a bloom filter, which makes it difficult for the hacker to determine the attributes for access. This improves the confidentiality of the data.

During break-glass access, the auxiliary message can only be viewed by either the CSP or the HC. The BGK is utilized for the retrieval of data from the CSP. The original data can be decrypted only by using an encapsulated password on the destination side. This mechanism protects the integrity of the data in emergency cases as well. Hence, in

this approach, in both the access schemes, the confidential data cannot be viewed, which provides the safe healthcare IoT with emergency access to save the patient's life.

3. Results and Discussion

In this, the proposed method is implemented using PBC with A-elliptic curve cryptography under a Windows 10 environment. The proposed method is evaluated using the following two terms:

- Communication overhead;
- Computational overhead.

These two metrics are analyzed for the proposed method and the process is compared with the existing lightweight break-glass access (LIBAC) and multi-authority MCP-ABE-BG approach.

3.1. Computational Overhead

In computational overhead, the execution time for generating the key, encrypting and decrypting the information, and the time taken for the break-glass key process is compared with the existing lightweight break-glass access (LIBAC) and multi-authority MCP-ABE-BG, as shown in the following figures.

3.1.1. Key Generation

Figure 6 shows the comparison of key generation time for different access schemes. It is observed that the time for generating keys increased concerning attributes. However, in multi-authority and attribute-based encryption, the key generation is four times higher than the proposed MCP-ABE-BG for 100 attributes. This shows that the proposed MCP-ABE-BG requires 0.8 s less to generate a key with 100 attributes.

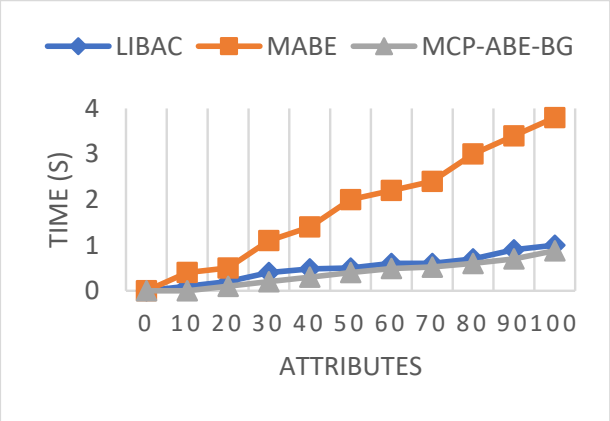

Figure 6. Key generation time comparison.

3.1.2. Encryption

Figure 7 shows the comparison of encryption generation for different access schemes. It is observed that the time for generating keys increased concerning attributes. However, in multi-authority and attribute-based encryption, the encryption time is nine times higher than the proposed MCP-ABE-BG for 100 attributes. This shows that the proposed MCP-ABE-BG requires 0.02 s less to encrypt the data with the generated key for 100 attributes.

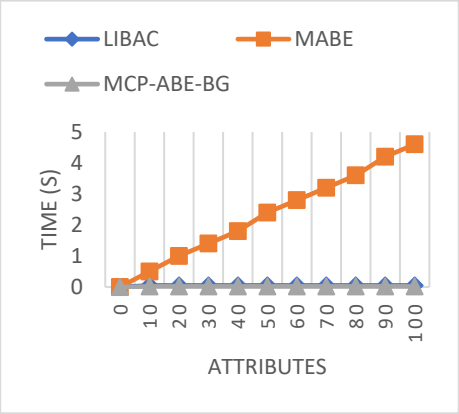

Figure 7. Encryption time comparison.

3.1.3. Decryption

Figure 8 shows the comparison of encryption generation for different access schemes. It is observed that the time for generating keys increased concerning attributes. Multi-authority and attribute-based encryption requires a longer time for decryption than the proposed MCP-ABE-BG for 100 attributes. This shows that the proposed MCP-ABE-BG utilizes the same amount of time as encryption for 100 attributes.

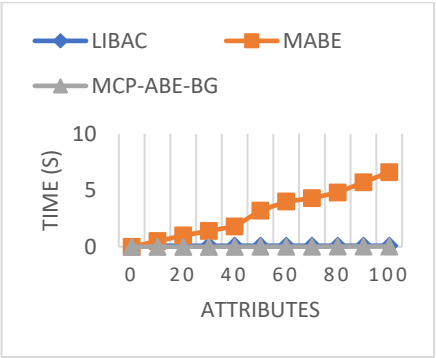

Figure 8. Decryption time.

3.1.4. Break-Glass Approach

In lightweight break-glass, the ECM requires 0.021S for performing the complete decryption with two hash functions. However, in the proposed method, the complete break glass process is performed within 0.018 s. This shows that the proposed MCP-ABE-BG requires minimal computational time compared to the multi-authority multi-ABE and lightweight break-glass approach. Therefore, the proposed method MCP-ABE-BG is computationally effective for the smart healthcare environment.

3.2. Communication Overhead

The sizes of the public key, private key, cipher text, and break key for the proposed method are compared with the existing lightweight break-glass access (LIBAC) and multi-authority MCP-ABE-BG, as shown in the following figures.

3.2.1. Public Key

Figure 9 shows the comparison of public key sizes using different access mechanisms. In LIBAC and MCP-ABE-BG, the public key size maintains a constant value of 0.256 kB and 0.896 kB, respectively, for all attributes. However, in the proposed MCP-ABE-BG, the key size, at both lower and higher attributes, is only 0.198 kB, which is minimal compared to the other two approaches.

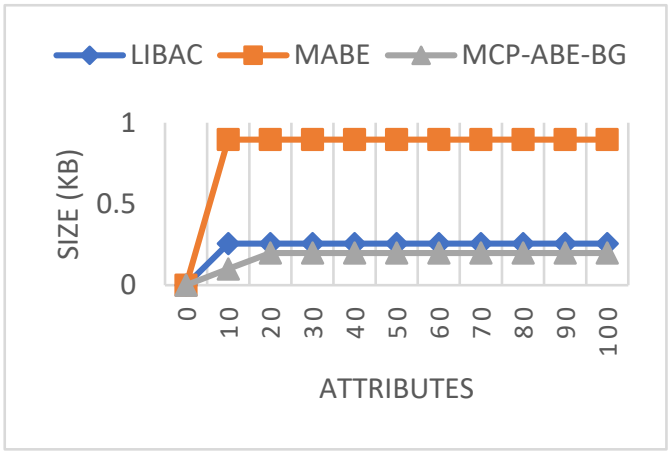

Figure 9. Public key size comparisons.

3.2.2. Private Key

Figure 10 shows that private key size increases along with the increase in attributes in all the approaches. However, in LIBAC and the proposed MCP-ABE-BG, the private key size is minimal as compared the MCP-ABE-BG approach. Especially notable, the proposed method's private key size is four times smaller than the MCP-ABE-BG key size for 100 attributes. This shows that the bloom filter helps to reduce the key size effectively.

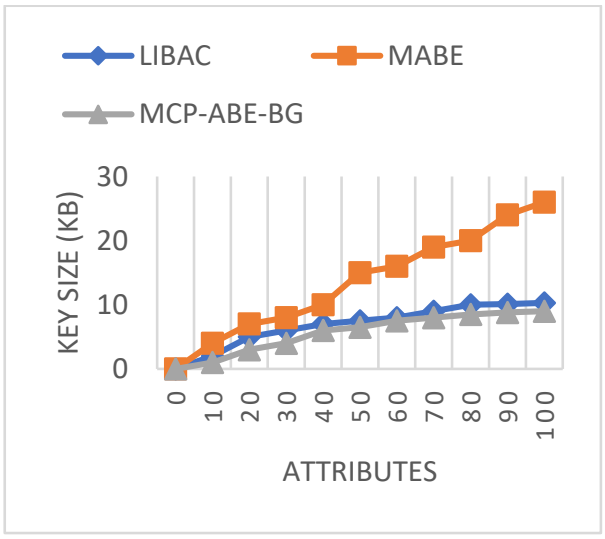

Figure 10. Private key size comparisons.

3.2.3. Cipher Text

Figure 11 shows the comparison of cipher text size for different access. In the MCP-ABE-BG approach, the cipher text size is linearly increased due to the increased private key size for attributes. However, in the proposed MCP-ABE-BG, the cipher text size is nine times the minimum of the MCP-ABE-BG approach and its size is 4% of the minimum of the LIBAC approach. This shows that the proposed approach requires less storage space in the cloud for saving protected electronic health records compared to other approaches.

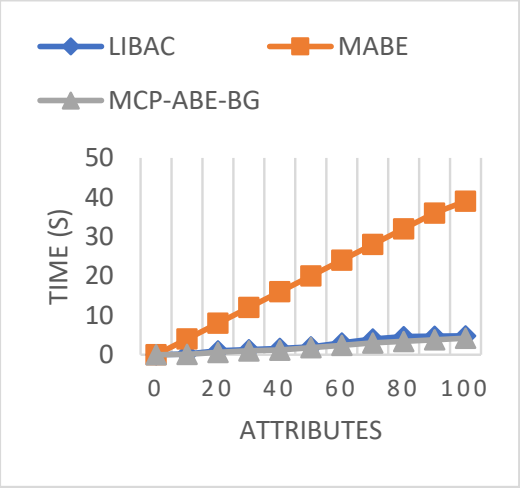

Figure 11. Cipher text size comparison.

3.2.4. Break-Glass Approach

In lightweight break-glass, the ECM generates a key measuring 0.256 kB for both public and private key processes. In multi-authority MCP-ABE-BG, break-glass access is not implemented. However, in the proposed method, the break-glass key size is reduced to 0.198 kB due to the bloom filter operation. This shows that the proposed MCP-ABE-BG requires minimum storage size compared to the multi-authority multi-ABE and lightweight break-glass approach. Therefore, the proposed method MCP-ABE-BG is computationally effective and requires less space for secure data transmission in the smart healthcare environment.

4. Conclusions

In this paper, a secured and dual-access scheme for the smart healthcare environment is proposed. Here, the modified CP-ABE is used during the normal data access period. The information is highly secured as compared to the traditional ABE because the access policy is verified using the bloom filter process instead of the tied access policy in the key generation and verification process. In emergency mode, the ECM can retrieve the information through the break-glass key from the shared password by patients. The experimental results show that the proposed approach is also best in terms of reduced overhead, compared to the lightweight break-glass protocol. The major advantage of this approach is that the key is not leaked at any stage, as it utilizes the bloom filter concept in the MCP-ABE process, which preserves the access policy and attributes. Therefore, the proposed MCP-ABE with break-glass is best for data access in smart healthcare to save patients' lives.

In the future, the proposed method can be improved by modifying the sharing scheme to limit the number of shares for the public key and extraction process.

Author Contributions: Conceptualization, C.R.B.D.; Methodology, N.K.A.; Validation, M.H.; Formal analysis, K.M.; Resources, D.R.S.V.; Data curation, K.P.R.; Visualization, M.T.B.O.; Supervision, H.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R125), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Data Availability Statement: The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Conflicts of Interest: There is no conflict of interest.

References

1. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164. [CrossRef]
2. Singh, J.; Pasquier, T.; Bacon, J.; Ko, H.; Eyers, D. Twenty security considerations for cloud-supported Internet of Things. *IEEE Internet Things J.* **2015**, *3*, 269–284. [CrossRef]
3. Gope, P.; Hwang, T. BSN-Care: A secure IoT-based modern healthcare system using body sensor network. *IEEE Sens. J.* **2015**, *16*, 1368–1376. [CrossRef]
4. Moosavi, S.R.; Gia, T.N.; Nigussie, E.; Rahmani, A.M.; Virtanen, S.; Tenhunen, H.; Isoaho, J. End-to-end security scheme for mobility enabled healthcare Internet of Things. *Future Gener. Comput. Syst.* **2016**, *64*, 108–124. [CrossRef]
5. Asplund, M.; Nadjm-Tehrani, S. Attitudes and perceptions of IoT security in critical societal services. *IEEE Access* **2016**, *4*, 2130–2138. [CrossRef]
6. Hossain, M.S.; Muhammad, G.; Rahman, S.M.M.; Abdul, W.; Alelaiwi, A. Toward end-to-end biomet rics-based security for IoT infrastructure. *IEEE Wirel. Commun.* **2016**, *23*, 44–51. [CrossRef]
7. Han, K.H.; Bae, W.S. Proposing and verifying a security-enhanced protocol for IoT-based communication for medical devices. *Clust. Comput.* **2016**, *19*, 2335–2341. [CrossRef]
8. Baker, S.B.; Xiang, W.; Atkinson, I. Internet of things for smart healthcare: Technologies, challenges, and opportunities. *IEEE Access* **2017**, *5*, 26521–26544. [CrossRef]
9. Mathur, A.; Newe, T.; Elgenaidi, W.; Rao, M.; Dooly, G. A secure end-to-end IoT solution. *Sens. Actuators A Phys.* **2017**, *263*, 291–299. [CrossRef]
10. Mahmood, Z.; Ning, H.; Ullah, A.; Yao, X. Secure authentication and prescription safety protocol for telecare health services using ubiquitous IoT. *Appl. Sci.* **2017**, *7*, 1069. [CrossRef]
11. Alkeem, E.A.; Shehada, D.; Yeun, C.Y.; Zemerly, M.J.; Hu, J. New secure healthcare system using cloud of things. *Clust. Comput.* **2018**, *20*, 2211–2229. [CrossRef]
12. Zhang, H.; Yu, J.; Tian, C.; Zhao, P.; Xu, G.; Lin, J. Cloud storage for electronic health records based on secret sharing with verifiable reconstruction outsourcing. *IEEE Access* **2018**, *6*, 40713–40722. [CrossRef]
13. Srinivas, J.; Das, A.K.; Kumar, N.; Rodrigues, J.J. Cloud centric authentication for wearable healthcare monitoring system. *IEEE Trans. Dependable Secur. Comput.* **2018**, *17*, 942–956. [CrossRef]
14. Yang, Y.; Zheng, X.; Guo, W.; Liu, X.; Chang, V. Privacy-preserving fusion of IoT and big data for e-health. *Future Gener. Comput. Syst.* **2018**, *86*, 1437–1455. [CrossRef]
15. Anaya, L.H.S.; Alsadoon, A.; Costadopoulos, N.; Prasad, P.W.C. Ethical implications of user perceptions of wearable devices. *Sci. Eng. Ethics* **2018**, *24*, 1–28. [CrossRef] [PubMed]